CLAIMS

1. A method for providing firewall fault tolerance in a network, the network including a plurality of firewalls, at least one server and at least one network flowswitch, the method comprising:

detecting in the network flowswitch an occurrence of a failed firewall of the plurality of firewalls;

detecting in the network flowswitch a packet from the server directed to the failed firewall after the occurrence of a failed firewall is detected;

changing a media access control (MAC) address of the packet with a MAC address of a functional firewall of the plurality of firewalls when the packet is detected; and

relaying the packet to the functional firewall after the MAC address is changed.

2. The method of claim 1 wherein the network comprises a plurality of servers.

3. The method of claim 2 wherein relaying the packet to the functional firewall comprises relaying the packet to the functional firewall over a media that is not shared with packets directed to other firewalls or servers.

4. The method of claim 1 wherein said detecting an occurrence of a failed firewall comprises sending a request to the plurality of firewalls, wherein an absence of a response from a particular firewall of the plurality of firewalls is indicative of a failure of the particular firewall.

5. The method of claim 1 wherein said detecting an occurrence of a failed firewall comprises sending at least one Address Resolution Protocol (ARP) request to each firewall of the plurality of firewalls, wherein an absence of a reply

to an ARP request from a particular firewall of the plurality of firewalls is indicative of a failure of the particular firewall.

6. The method of claim 1 further comprising:

detecting an address resolution protocol (ARP) request from the server to the failed firewall; and

responding to the ARP request with the MAC address of the functional firewall, whereby the server is configured to send subsequent outbound packets with the MAC address of the functional firewall.

7. The method of claim 1 wherein said detecting an occurrence of a failed firewall comprises sending ICMP echo packets to each firewall of the plurality of firewalls and wherein an absence of a response from a particular firewall of the plurality of firewalls during a predetermined interval is indicative of a failure of the particular firewall.

8. The method of claim 1 further comprising:

detecting a recovery of the failed firewall, the failed firewall becoming a recovered firewall; and

terminating said detecting a packet from the server directed to the failed firewall when said failed firewall recovers.

9. The method of claim 8 further comprising waiting for a time out period to expire after said detecting when the failed firewall recovers.

10. The method of claim 9 wherein the time out period is greater than or equal to a time period needed for the recovered firewall to learn routes to all known clients.

11. The method of claim 8 wherein said detecting a recovery of the failed firewall comprises sending to the failed firewall a request and a response from the failed firewall is indicative of a recovery of the failed firewall.

12. The method of claim 8 wherein said detecting a recovery of the failed firewall comprises detecting a a packet from the failed firewall in response to a request.

13. The method of claim 8 wherein said detecting a recovery of the failed firewall comprises sending ARP requests to each firewall of the plurality of firewalls, wherein an occurrence of a reply to an ARP request from the failed firewall is indicative of a recovery of the failed firewall.

14. The method of claim 1 wherein packets are transferred between the server and a firewall of the plurality of firewalls through a switch circuit.

15. The method of claim 14 wherein the switch circuit comprises a switched Ethernet circuit.

16. An apparatus for providing firewall fault tolerance in a network, the network including a plurality of firewalls, at least one server and at least one network flowswitch, the apparatus comprising:

means for detecting an occurrence of a failed firewall in the plurality of firewalls;

means for detecting a packet from the server directed to the failed firewall after the failed firewall is detected;

means for changing a media access control (MAC) address of the packet with a MAC address of a functional firewall of the plurality of firewalls when the packet is detected; and

means for relaying the packet to the functional firewall after the MAC address is changed.

17. The apparatus of claim 16 further comprising:

means for detecting an address resolution protocol (ARP) request from the server to the failed firewall; and

means for responding to the ARP request with the MAC address of the functional firewall, wherein the server sends subsequent outbound packets with the MAC address of the functional firewall.

18. The apparatus of claim 16 wherein said means for detecting a failed firewall comprises means for transmitting a request to the plurality of firewalls, wherein an absence of a reply from a particular firewall of the plurality of firewalls is indicative of a failure of the particular firewall.

19. The apparatus of claim 16 wherein said means for detecting a failed firewall comprises means for sending ARP requests to each firewall of the plurality of firewalls, wherein an absence of a reply to an ARP request from a particular firewall of the plurality of firewalls is indicative of a failure of the particular firewall.

20. The apparatus of claim 16 further comprising:

means for detecting a recovery of the failed firewall, the failed firewall becoming a recovered firewall; and

means for disabling said means for detecting a packet from the server directed to the failed firewall when said failed firewall recovers.

21. The apparatus of claim 20 wherein said means for detecting a recovery of the failed firewall comprises means for transmitting a request to the plurality of firewalls, wherein a response from the failed firewall is indicative of recovery of the failed firewall.

22. The apparatus of claim 16 wherein said means for detecting a recovery of the failed firewall comprises means for sending ARP requests to each firewall of the plurality of firewalls, wherein an occurrence of a reply to an ARP request from the failed firewall is indicative of a recovery of the failed firewall.

23. A network having firewall fault tolerance, the network configured to be coupled to a network backbone, the network comprising:

a switch circuit;

a first firewall coupled to said switch circuit and the network backbone, said first firewall having a media access control (MAC) address;

a second firewall coupled to said switch circuit and the network backbone, said second firewall having a MAC address; and

a server coupled to the switch circuit,

wherein the switch circuit is configured to detect when the first firewall fails, the switch circuit being further configured to monitor packets sent by the server to the first firewall and to change in the packet the MAC address of the first firewall to the MAC address of the second firewall.

24. The network of claim 23 further comprising a plurality of servers, the plurality of servers including the server.

25. The network of claim 23 wherein the switch circuit is further configured to relay the packet to the second firewall after changing the MAC address of the first firewall to the MAC address of the second firewall.

26. The network of claim 23 wherein the switch circuit is configured to detect a failed firewall by transmitting a request to the first and second firewalls, wherein an absence of a reply from a particular firewall of the first and second firewalls is indicative of a failure of the particular firewall.

27. The network of claim 23 wherein the switch circuit is configured to detect a failed firewall by sending ARP requests to the first and second firewalls, wherein an absence of a reply to an ARP request from a particular firewall of the first and second of firewalls is indicative of a failure of the particular firewall.

28. The network of claim 23 wherein the switch circuit is configured to detect a failed firewall by sending ICMP echo requests to the first and second firewalls, wherein an absence of a reply to an ICMP echo request from a particular firewall of the first and second of firewalls is indicative of a failure of the particular firewall.

29. The network of claim 23 wherein the switch circuit is configured to detect a failed firewall by monitoring responses from the firewalls to requests sent at predetermined intervals.

30. The network of claim 23 wherein the switch circuit is further configured to:

detect an address resolution protocol (ARP) request from the server to the first firewall; and

respond to the ARP request with the MAC address of the second firewall, whereby the server sends subsequent outbound packets with the MAC address of the second firewall.

31. The network of claim 23 wherein the switch circuit is further configured to:

detect when the first firewall recovers; and

terminate monitoring for packets sent by the server to the first firewall after the first firewall recovers.

32. The network of claim 31 wherein the switch circuit is further configured to wait for a time-out period to expire after detecting when the first firewall recovers.

33. The network of claim 32 wherein the time-out period is greater than or equal to a time period needed for the recovered first firewall to learn routes to all known clients.

34. The network of claim 31 wherein the switch circuit is configured to detect a recovery of the failed firewall by transmitting a request to the first and second firewalls, wherein receipt of a response from the failed firewall is indicative of a recovery of the failed firewall.

35. The network of claim 31 wherein the switch circuit is configured to detect a recovery of the failed firewall by sending ARP requests to the first and second firewalls, wherein an occurrence of a reply to an ARP request from the failed firewall is indicative of a recovery of the failed firewall.

36. The network of claim 31 wherein the switch circuit is configured to detect a recovery of the failed firewall by sending ICMP echo requests to the first and second firewalls, wherein an occurrence of a reply to an ICMP echo request from the failed firewall is indicative of a recovery of the failed firewall.

37. The network of claim 23 wherein packets are transferred between the server and the first firewall through the switch circuit and between the server and the second firewall through the switch circuit.

38. The network of claim 36 wherein the switch circuit is configured to provide full duplex communication between the first firewall and the server.

39. The network of claim 36 wherein the switch circuit comprises a switched Ethernet circuit.

40. A method for providing fault tolerance in a network, the network including a plurality of firewalls, the method comprising:

generating a request message on a first side of a first firewall in the plurality of firewalls;

sending the request message through the first firewall to a second side of the first firewall; and

processing an absence of a reply from the second side to the request message as a failure of the first firewall.

41. The method of Claim 40 further comprising:

maintaining in a first memory on said first side a first functional status for each firewall;

maintaining in a second memory on said second side a second functional status for each firewall; and

wherein said first functional status is identical to said second functional status.

42. The method of Claim 41 further comprising:

maintaining session information in a firewall for each session between computers separated by the firewall.

43. The method of Claim 40 further comprising:

sending the request message through the first firewall to a third side of the first firewall; and

processing an absence of a reply from the third side to the request message as a failure of the first firewall.

44. The method of Claim 40 wherein:

the generating, sending and processing are performed in a switch circuit.

45. The method of Claim 40 further comprising:

performing Network Address Translation (NAT) in the first firewall; and

adding a rule in the first firewall to maintain unchanged an internet protocol (IP) address of a source of the request message.

46. The method of Claim 40 further comprising:

receiving a request on a port; and

sending a reply on said port.

47. A network having fault tolerance, the network comprising:

a first switch circuit;

a second switch circuit; and

a plurality of firewalls coupled to each of the first switch circuit and the second switch circuit, each firewall being coupled to the first switch circuit by a first medium that is not shared with another firewall in the plurality of firewalls and each firewall is coupled to the second switch circuit by a second medium that is not shared with another firewall in the plurality of firewalls.

48. The network of Claim 47 further comprising:

a plurality of computers, each computer being coupled to the first switch circuit, each computer being configured with a media access control (MAC) address of a predetermined firewall in the plurality of firewalls, the predetermined firewall being a default gateway for transferring packets outside the network.

Rule 1.126

49. The network of Claim 47, wherein the computers are hereinafter "first computers", the network further comprising:

a plurality of second computers, each second computer being coupled to the first switch circuit, each computer being configured with a MAC address of a

predetermined firewall in the plurality of firewalls, the predetermined firewall being a default gateway for transferring packets outside the network.

49. The network of Claim 47 further comprising:

a plurality of routers coupled to the second switch circuit.

50. The network of Claim 47 wherein each of the first switch circuit and the second switch circuit comprises:

a first storage element encoded with a list of the plurality of firewalls; and

a second storage element encoded with an identity of a firewall in the plurality as a replacement firewall for any other firewall in the plurality that has failed.

51. The network of claim 47 wherein:

each of the first switch circuit and the second switch circuit is configured to send a request message to the other of the first switch circuit and the second switch circuit; and

each of the first switch circuit and the second switch circuit is configured to treat absence of a response to the request message as a failure of a firewall through which the request message was sent.

52. The network of Claim 51 wherein:

the request message conforms to an internet protocol selected from the group consisting of:

(a) ping;

(b) address resolution protocol (ARP); and

(c) internet message control protocol (ICMP).

53. The network of Claim 47 wherein:

the first switch circuit transfers a plurality of packets to a first firewall in the plurality of firewalls through a first medium without changing any portion of any packet in the plurality of packets while the first firewall is functional.

54. The network of Claim 47 wherein:

the first switch circuit replaces in each packet (hereinafter "modified packet") a media access control (MAC) address of the first firewall with a MAC address of a second firewall in the plurality of firewalls and transfers each modified packet to the second firewall while the first firewall is nonfunctional.

55. The network of claim 47 wherein the switch circuit comprises a switched Ethernet circuit.

56. A method for providing fault tolerance in a network, the network including a plurality of firewalls, the method comprising:

detecting a failure of a first firewall in the plurality of firewalls; and

replacing, in a packet, a media access control (MAC) address of the first firewall with a MAC address of a second firewall in the plurality of firewalls in response to the failure.

57. The method of Claim 56 wherein:

the detecting is performed in a switch circuit.

58. The method of Claim 56 further comprising:

receiving the packet after detecting the failure and prior to the replacing.

59. The method of claim 56 further comprising:

transferring a plurality of packets other than the packet, between a host and a firewall in the plurality of firewalls through a switch circuit.

60. The method of Claim 59 wherein:

each of the packets contains an internet protocol (IP) address; and

the method does not change the IP address during transferring of the packets to any of the firewalls.

62

61. The method of Claim 59 wherein:

the IP address is hereinafter "first IP address";

each of the firewalls has a first side; and

each of the firewalls has the first IP address on the first side.

63

62. The method of Claim 59 wherein:

the method does not change the MAC address of any of the packets during the transferring, until the detecting of failure.